

REMARKS

In the Office Action, the Examiner rejected claims 1–20. By way of this response, Applicants have amended claim 1 to more clearly set forth certain aspects. Claims 1–20 remain pending in the present application and are believed to be in condition for allowance. In view of the following remarks, the Applicants respectfully request reconsideration and allowance of all pending claims.

Claim Rejections under 35 U.S.C. § 103(a)

In the Office Action the Examiner rejected claims 1-20 under 35 U.S.C. §103(a) as being unpatentable over Saarinen (Publication No.: U.S. 2002/0172359 A1, hereafter Saarinen) in view of Kara (U.S. Patent No. 5,802,175; hereinafter Kara) and Nordqvist et al. (Publication No.: U.S. 2002/0191799 A1, hereafter Nordqvist). Applicants respectfully traverse these objections.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d. 1430 (Fed. Cir. 1990). Accordingly, to establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). The Examiner must provide objective evidence, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to

combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). Moreover, a statement that the proposed modification would have been “well within the ordinary skill of the art” based on individual knowledge of the claimed elements cannot be relied upon to establish a *prima facie* case of obviousness without some *objective reason to combine* the teachings of the references. *Ex parte Levengood*, 28 U.S.P.Q.2d 1300 (B.P.A.I. 1993); *In re Kotzab*, 217 F.3d 1365, 1371, 55 U.S.P.Q.2d. 1313, 1318 (Fed. Cir. 2000); *Al-Site Corp. v. VSI Int’l Inc.*, 174 F.3d 1308, 50 U.S.P.Q.2d. 1161 (Fed. Cir. 1999).

Additionally, the pending claims must be given an interpretation that is reasonable and consistent with the *specification*. See *In re Prater*, 415 F.2d 1393, 1404-05, 162 U.S.P.Q. 541, 550-51 (C.C.P.A. 1969) (emphasis added); see also *In re Morris*, 127 F.3d 1048, 1054-55, 44 U.S.P.Q.2d 1023, 1027-28 (Fed. Cir. 1997); see also M.P.E.P. §§ 608.01(o) and 2111. Indeed, the specification is “the primary basis for construing the claims.” See *Phillips v. AWH Corp.*, No. 03-1269, -1286, at 13-16 (Fed. Cir. July 12, 2005) (*en banc*). One should rely *heavily* on the written description for guidance as to the meaning of the claims. See *id.*

Furthermore, interpretation of the claims must also be consistent with the interpretation that *one of ordinary skill in the art* would reach. See *In re Cortright*, 165 F.3d 1353, 1359, 49 U.S.P.Q.2d 1464, 1468 (Fed. Cir. 1999); M.P.E.P. § 2111. “The inquiry into how a person of ordinary skill in the art understands a claim term provides an objective baseline from which to begin claim interpretation.” See *Collegenet, Inc. v. ApplyYourself, Inc.*, No. 04-1202, -1222, 1251, at 8-9 (Fed. Cir. August 2, 2005) (quoting *Phillips*, No. 03-1269, -1286, at 16). The Federal Circuit has made clear that derivation of a claim term must be based on “usage in the ordinary and accustomed meaning of the words amongst artisans of ordinary skill in the relevant art.” See *id.*

Independent Claim 1 Recites Features Omitted from Saarinen, Kara, and Nordqvist

Independent claim 1 recites, *inter alia*: “remotely storing *a seed pool backup of the seed pool* via a network; and restoring the seed pool backup via the network to local memory following a power loss event causing loss to the seed pool.” (Emphasis added). The Applicants respectfully assert that nothing in Saarinen, Kara and Nordqvist teaches or suggests, alone or in hypothetical combination, all of the features recited above.

In the Office Action, the Examiner admits that Saarinen does not explicitly teach remotely storing a seed pool, and further admits that Saarinen and Kara do not disclose restoring the seed pool backup to local memory. Applicants agree that such subject matter is absent from the references, and further assert that none of the references disclose a backup seed pool of the seed pool. Specifically, Saarinen discloses a cryptographic method and apparatus for generating a pseudo-random number. *See Saarinen*, paragraph 1. As a part of the method, there is a reseeding of a pseudo-random number generator (“PRNG”) to change the state of the PRNG. *Id.* at paragraphs 22 and 71. However, there is no mention of a seed pool backup, much less a remotely stored seed pool backup. Therefore, in addition to the deficiencies recognized by the Examiner, Saarinen fails to disclose a remotely stored seed pool backup of the seed pool as recited in claim 1.

Kara fails to obviate this deficiency of Saarinen. Specifically, the Kara reference discloses the use of a single seed stored on a portable memory device for use in a cryptographic system. *See Kara*, col. 2, ll. 44-46 and col. 6, ll. 3-7. The portable memory device may be coupled to a host via a network to supply the key to the host. *See id.* at col. 2, ll. 44-46 and col. 3, ll. 51-56. Additionally, in an alternative embodiment, information from the host may be used for seeding a randomizer in the portable memory. *Id.* at col. 6, ll. 8-15. The information from the host and from the portable memory are combined to seed a random sequence generator. *Id.* at col. 6, lines 8-40. A subsequently generated cryptographic key is then stored on the portable memory device. *Id.* However,

no backup is ever made of the seed. Therefore, Kara discloses only a single seed, and not a seed pool backup of the seed pool as recited in claim 1.

Additionally, Nordqvist fails to obviate the deficiencies of both Saarinen and Kara. In sharp contrast to the Examiner's assertion that Nordqvist discloses restoring a seed pool backup, Nordqvist does not even mention seed pools much less *a seed pool backup*. Nordqvist is directed to hearing aids and the section of Nordqvist relied upon by the Examiner refers to algorithm parameters for controlling certain characteristics such as corner frequencies and slopes of filters, etc. *See Nordqvist*, paragraph 22. These parameter values may be associated with subroutines wherein the user may select from among various preset programs in accordance with his/her preferences. *See id.* at paragraphs 21-22. Initial parameter values are stored in non-volatile memory to allow them to be retained during power supply interruptions, but they are never used in a seeding capacity and cannot reasonably be considered a seed pool. *See id.* These parameters, therefore, do not make up a seed pool, much less a seed pool backup as recited in claim 1. As such, Nordqvist fails to obviate the deficiencies of Saarinen and Kara in at least this respect. Therefore, Saarinen, Kara and Nordqvist, alone or in hypothetical combination, do not disclose all of the elements of claim 1.

Moreover, the claims depending from independent claim 1 recite subject matter not found in any of the references cited by the Examiner. For example, claim 2 recites *inter alia*, "*periodically storing the seed pool backup on a remote storage device.*" (Emphasis added). Claim 4 recites, *inter alia*, "*modifying the seed pool backup with additional random bits.*" (Emphasis added). Claim 10 recites, *inter alia*, "*transmitting the seed pool backup from remote storage to the local memory via the network following a battery replacement for the local memory.*" (Emphasis added). In addition to reciting unique subject matter not found in any of the cited references, these dependent claims give insight into the nature of the claimed embodiment of the invention.

Because the references relied upon by the Examiner do not include all of the claimed elements, either alone or in hypothetical combination, Applicants respectfully request withdrawal of the rejections under 35 U.S.C. §103(a) for independent claim 1. Additionally, Applicants request withdrawal of the Examiner's rejection of the claims dependent from independent claim 1 in view of their respective dependencies and in view of unique matter recited in each dependent claim.

Independent Claim 11 Recites Features Omitted from Saarinen, Kara, and Nordqvist

Independent claim 11 recites, *inter alia*:

A method of restoring a seed pool for generating a random number for a security system, the method comprising the acts of: transmitting a *periodically stored backup of the seed pool* to the security system via a network following loss of the seed pool from the security system; and repopulating local memory of the security system with the periodically stored backup for use in generating the random number.

(Emphasis added). The Applicants respectfully assert that none of the references, alone or in hypothetical combination, disclose all of the features recited above.

In the Office Action, the Examiner admits that Saarinen does not explicitly teach remotely storing a seed pool, and further admits that Saarinen and Kara do not disclose repopulating local memory with the stored backup. Applicants agree that such subject matter is absent from the references, and further assert that none of the references disclose a backup of the seed pool, much less a *periodically stored backup of the seed pool* as recited in claim 11. Specifically, as described above with reference to claim 1, Saarinen discloses a PRNG that is re-seeded. *See Saarinen*, at paragraphs 22 and 71. However, there is no mention of a seed pool backup. Therefore, in addition to the deficiencies recognized by the Examiner, Saarinen fails to disclose a *periodically stored backup of the seed pool* as recited in claim 11.

Kara fails to obviate this deficiency of Saarinen. Specifically, the Kara reference does not even mention a backup of the seed pool, much less a periodically stored backup of the seed pool. In sharp contrast to claim 11, the Kara reference discloses supplying a seed, originating on a portable memory device, to a key generation program. *See Kara*, col. 2, ll. 44-46 and col. 6, ll. 3-7. As discussed above in reference to claim 1, no backup of original seeds are ever created or even mentioned in Kara. Therefore, there is no backup of the seed pool. For at least this reason, therefore, Kara does not cure the deficiencies of Saarinen.

Nordqvist fails to obviate the deficiencies of both Saarinen and Kara. In sharp contrast to the Examiner's assertion that Nordqvist discloses restoring a seed pool backup, Nordqvist does not even mention seed pools much less a periodically stored backup of a seed pool. As discussed above, Nordqvist is directed to hearing aids and the section of Nordqvist relied upon by the Examiner refers to algorithm parameters for controlling certain characteristics such as corner frequencies and slopes of filters, etc. *See Nordqvist*, paragraph 22. Initial parameter values are stored in non-volatile memory to allow them to be retained during power supply interruptions, but they still are never used in a seeding capacity and cannot reasonably be considered a seed pool. *See id.* Therefore, Nordqvist does not disclose a periodically stored backup of the seed pool as recited in claim 11 and fails to obviate the deficiencies of Saarinen and Kara in at least this respect.

In addition to not disclosing anything related to a seed pool, the Nordqvist reference never stores anything remotely or transmits anything via a network. As mentioned previously, the Nordqvist reference is directed to hearing aids. Hearing aids are not subject to security issues that necessitate cryptographic techniques. Furthermore, they are never connected to networks to enable remote storage and transmission of seed pools. As such, the initial parameters stored in non-volatile memory are local to the hearing aid devices. Furthermore, the initial values are not periodically stored nor ever

altered, but rather are permanently stored to be used in the event of power loss. *See Nordqvist*, paragraph 23. Therefore, in addition to the aforementioned reasons, the Nordqvist reference fails to obviate the deficiencies of Saarinen and Kara by not disclosing a periodically stored backup seed pool.

Additionally, similar to the claims depending from claim 1, the claims depending from claim 11 further set forth unique elements that further distinguish the claims over the cited art. Specifically, for example, claim 12 recites, *inter alia*, “modifying the periodically stored backup with additional random bits.” Applicants assert that none of the references, alone or in combination, disclose such subject matter.

For at least the reasons mentioned above, Applicants request withdrawal of the Examiner’s rejection of independent claim 11 and further request the withdrawal of all claims dependent therefrom in view of their respective dependencies and in view of unique matter recited in each dependent claim.

Independent Claim 17 Recites Features Omitted from Saarinen, Kara, and Nordqvist

Independent claim 17 recites, *inter alia*:

a seed pool stored on the power dependent memory device, wherein the seed pool comprises a plurality of random bits; . . . a backup control module configured for *periodically storing a backup of the seed pool* in the remote storage device; and a restoration control module configured for repopulating the power dependent memory device with the backup following replacement of the limited life battery.

(Emphasis added). The Applicants respectfully assert that the cited reference, taken alone or in hypothetical combination, fail to disclose all the elements recited in independent claim 17.

In the Office Action, the Examiner admits that Saarinen does not explicitly teach remotely storing a seed pool, and further admits that Saarinen and Kara do not disclose

repopulating local memory with the stored backup. Applicants agree that such subject matter is absent from the references, and further assert that none of the references disclose a backup of the seed pool, much less a *periodically stored backup of the seed pool* as recited in claim 17. Specifically, as described above with reference to claim 1, Saarinen discloses a PRNG that is re-seeded. *See Saarinen*, at paragraphs 22 and 71. However, there is no mention of a seed pool backup. Therefore, in addition to the deficiencies recognized by the Examiner, Saarinen fails to disclose a *periodically stored backup of the seed pool* as recited in claim 17.

Kara fails to obviate this deficiency of Saarinen. Specifically, the Kara reference does not ever mention a *backup of the seed pool*, much less a *periodically stored backup of the seed pool*. In sharp contrast to claim 17, the Kara reference discloses supplying a seed, originating on a portable memory device, to a key generation program. *See Kara*, col. 2, ll. 44-46 and col. 6, ll. 3-7. As discussed above in reference to claim 1, no backup of original seeds are ever created or even mentioned in Kara. Therefore, there is no backup of the seed pool. For at least this reason, therefore, Kara does not cure the deficiencies of Saarinen.

Nordqvist fails to obviate the deficiencies of both Saarinen and Kara. In sharp contrast to the Examiner's assertion that Nordqvist discloses restoring a seed pool backup, Nordqvist does not even mention seed pools much less a periodically stored backup of a seed pool. As discussed above, Nordqvist is directed to hearing aids and the section of Nordqvist relied upon by the Examiner refers to algorithm parameters for controlling certain characteristics such as corner frequencies and slopes of filters, etc. *See Nordqvist*, paragraph 22. Initial parameter values are stored in non-volatile memory to allow them to be retained during power supply interruptions, but they still are never used in a seeding capacity and cannot reasonably be considered a seed pool. *See id.* Therefore, Nordqvist does not disclose a *periodically stored backup of the seed pool* as

recited in claim 17 and fails to obviate the deficiencies of Saarinen and Kara in at least this respect.

In addition to not disclosing anything related to a seed pool, the Nordqvist reference never stores anything remotely or transmits anything via a network. As mentioned previously, the Nordqvist reference is directed to hearing aids. Hearing aids are not subject to security issues that necessitate cryptographic techniques. Furthermore, they are never connected to networks to enable remote storage and transmission of anything. As such, the initial parameters stored in non-volatile memory are local to the hearing aid devices. Furthermore, the initial values are not periodically stored, but rather are permanently stored to be retained in the event of power loss. *See Nordqvist*, paragraph 23. Therefore, in addition to the aforementioned reasons, the Nordqvist reference fails to obviate the deficiencies of Saarinen and Kara by not disclosing a periodically stored backup seed pool.

In addition to the above mentioned elements absent from the cited references, none of the references disclose a backup control module and a restoration control module. As indicated earlier, claim 17 recites, *inter alia*, a backup control module for periodically storing a backup of the seed pool and a restoration control module for repopulating a memory device with the backup. In the absence of any backup of a seed pool it is impossible for the references to have such modules and Applicants assert that such elements are absent from any of the cited references. Therefore, for this additional reason, the references fail to disclose all the elements of the present invention.

Additionally, similar to the claims depending from claims 1 and 11, the claims depending from claim 17 further set forth unique elements that distinguish the claims over the cited art. Specifically, for example, claim 19 recites, *inter alia*, “a seed pool modification module configured for capturing one or more bits of data from a hardware

component and adding the one or more bits to the backup.” None of the cited references disclose these elements of claim 19.

In light of the foregoing discussion, the Applicants respectfully request withdrawal of the rejection of independent claim 17 and further request the withdrawal of all claims dependent therefrom based on their dependencies.

Improper Combination - Lack of Objective Evidence of Reasons to Combine

In addition, the Examiner has not shown the requisite motivation or suggestion to modify or combine the cited references to reach the present claims. As summarized above, the Examiner must provide objective evidence, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). In the present rejection, the Examiner combined the cited references based on the *conclusory and subjective statement*:

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup data during battery replacement or power/data loss. One would have been motivated to incorporate the teachings of bucking up [*sic*] data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2, par. 0023).

Office Action, pages 3, 5 and 6. Accordingly, Applicants challenge the Examiner to produce *objective evidence* of the requisite motivation or suggestion to combine the cited references, or remove the foregoing rejection under 35 U.S.C. § 103.

As briefly mentioned earlier, Nordqvist is related to hearing aids while Saarinen and Kara are related to cryptographic systems. There is nothing in Nordqvist even remotely related to seed pools or even cryptography. The parameters cited to by the

Examiner are never used to encode a cryptographic key or in the generation of a pseudo-random number. The parameters are simply used as controls for algorithms related to how sound is processed by the hearing aid. *See Nordqvist*, at paragraphs 22-23. Therefore, for at least this reason, the hypothetical combination of Saarinen, Kara and Nordqvist is improper.

For the reasons discussed in detail above, Applicants request the withdrawal of the rejections of independent claims 1, 11 and 17 as well as the withdrawal of the rejection of all claims dependent therefrom.

Request Evidence to Support Official Notice

In the context of seed pools, the Examiner states, “it is well known to backup a data during battery replacement or power/data loss.” Office Action, pages 3, 5 and 6 (emphasis added). Again, only the Saarinen and Kara references relate to seed, whereas the Nordqvist reference is absolutely unrelated to seed pools. The Examiner appears to be filling a substantial gap without any evidentiary support. Essentially, the Examiner has taken Official Notice of facts outside of the record that the Examiner apparently believes are capable of demonstration as being “well-known” in the art. Therefore, in accordance with M.P.E.P. § 2144.03, the Applicants hereby seasonably traverse and challenge the Examiner’s use of Official Notice. Furthermore, Applicants emphasize that the “well-known” facts asserted by the Examiner are not of a “notorious character” and are clearly not “capable of such instant and unquestionable demonstration as to defy dispute.” *See* M.P.E.P. § 2144.03. Specifically, the Applicants respectfully request that the Examiner produce evidence in support of the Examiner’s position as soon as practicable during prosecution and that the Examiner add a reference to the rejection in the next Official Action. If the Examiner finds such a reference and applies it in combination with the presently cited references, the Applicants further request that the Examiner specifically identify the portion of the newly cited reference that discloses the

allegedly “well known” elements of the instant claim, as discussed above, or withdraw the rejection.

In addition, the Applicants submit that the Examiner’s use of Office Notice is improper on a legal basis, because the Office Notice is a broad sweeping statement regarding features of all pending claims. Section 2144.03 of the Manual of Patent Examining Procedure specifically states:

In **limited circumstances**, it is appropriate for an examiner to take office notice of facts not in the record or to rely on “common knowledge” in making a rejection, however such rejections should be **judiciously applied**.

...

Office notice without documentary evidence to support an examiner’s conclusion is permissible only in some circumstances. While “office notice” may be relied on, these **circumstances should be rare** when an application is under final rejection or action under 37 CFR 1.113.

...

As noted by the court in *In re Ahlert*, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of facts beyond the record which may be taken by the examiner must be “**capable of such instant and unquestionable demonstration as to defy dispute**” (citing *In re Knapp Monarch Co.*, 296 F.2d 230, 132 USPQ 6 (CCPA 1961)).

...

For example, assertions of technical facts in the areas of esoteric technology or **specific knowledge of the prior art must always be supported by citation to some reference work** recognized as standard in the pertinent art. *In re Ahlert*, 424 F.2d at 1091, 165 USPQ at 420-21.

...

In re Eynde, 480 F.2d 1364, 1370, 178 USPQ 470, 474 (CCPA 1973) (“[W]e reject the notion that judicial or administrative notice may be taken of the state of the art. The **facts constituting the state of the art** are normally subject to the possibility of rational disagreement among reasonable men and are **not amenable to the taking of such notice.**”).

...

Furthermore, as noted by the court in *Ahlert*, any facts so noticed should be of notorious character and **serve only to "fill in the gaps" in an insubstantial manner** which might exist in the evidentiary showing made by the examiner to support a particular ground for rejection.

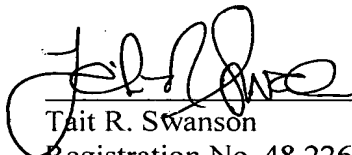
M.P.E.P. (Rev. 2, May 2004) § 2144.03, Pages 2100-136-138. In view of these passages, the Applicants reiterate that the Examiner's use of Office Notice is improper and cannot stand, because the scope of the Office Notice is far beyond an *insubstantial gap* in the cited reference. Moreover, the Examiner's Office Notice refers to the *general state of the art*, which the foregoing legal precedent clearly precludes.

Conclusion

The Applicants respectfully submit that all pending claims should be in condition for allowance. However, if the Examiner believes certain amendments are necessary to clarify the present claims or if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: December 19, 2005


Tait R. Swanson
Registration No. 48,226
(281) 970-4545

HEWLETT-PACKARD COMPANY

Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400